Starling Cloud-Plattform von One Identity (OI)

Enterprise Zugriffsmanagement für die Cloud

Die Nutzung sowohl von on-premise Softwarelösungen als auch cloudbasierter Anwendungen ist in den Unternehmen heutzutage Realität. Doch was bedeutet das für ein sicheres Zugriffsmanagement im Sinne der Identity Governance & Administration (IGA)? Eine Universallösung gibt es nicht, denn der Weg eines jeden Unternehmens hin zur Nutzung der Cloudtechnologie ist höchst individuell. Die Starling Plattform von One Identity schafft die technischen und administrativen Voraussetzungen für eine unternehmensspezifische Lösung, die sicherstellt, dass auch in einer hybriden Systemumgebung aktuelle IT-Sicherheitsvorgaben eingehalten werden.

Sichere Integration von cloudbasierten Diensten

Erfolgreich auf dem Markt agierende Unternehmen müssen zunehmend flexibel auf aktuelle Anforderungen reagieren können. Eine cloudbasierte IT-Infrastruktur beinhaltet in der Regel Speicherplatz, Rechenleistung oder auch Anwendungssoftware und ermöglicht es Unternehmen, bedarfsorientiert und ressourcenschonend auf sich verändernde Rahmenbedingungen zu reagieren. Untrennbar damit verbunden ist das Thema der IT-Security, denn in der Regel greifen zahlreiche Nutzer auf eine Cloud zu. Die Verschlüsselung der abgelegten Daten sowie eine Zugriffs- bzw. Rechtekontrolle sind deshalb unabdingbar. One Identity stellt die nötigen Konnektoren zur Integration der verschiedenen Systeme bereit und bietet diverse Services an, um die Zugriffssicherheit z. B. durch Zwei-Faktor-Authentifizierung und das automatisierte Management von Zugriffsanfragen oder -zertifizierungen maßgeblich zu erhöhen.

Konnektivität ist Trumpf

Die Zahl der genutzten Systeme und Anwendungen in einem Unternehmen ist oftmals immens. Um die Produktivität der Mitarbeiter auch während der Implementierung eines neues professionellen Identitäts- und Zugriffsmanagements zu gewährleisten, ist es deshalb wichtig, dass sämtliche Applikationen möglichst schnell und unkompliziert integriert werden können. One Identity hält zu diesem Zweck eine Vielzahl von Konnektoren bereit, welche die unterschiedlichen Schnittstellen und Standards bedienen. So können z. B. Berechtigungsanforderungen oder Zugriffszertifizierungen zentral und über die gesamte Systemlandschaft hinweg gemanagt werden.

Starker Zugriffsschutz dank Zwei-Faktor-Authentifizierung

Ein hohes Sicherheitsrisiko für Unternehmen stellen grundsätzlich auch kompromittierte Kennwörter dar. Zum Schutz vor Datensicherheitsverletzungen können Organisationen mittels der sogenannten Zwei-

Faktor-Authentifizierung eine möglichst starke Authentifizierung beim Zugriff auf die Unternehmenssysteme etablieren. Die SaaS-basierte Lösung von One Identity bietet verschiedene Authentifizierungsmethoden an. Benutzer können z. B. mithilfe der mobilen App für iOS, Android und Chrome Initialpasswörter generieren oder sich Einmal-Kennwörter per SMS oder Telefonanrufen zusenden lassen. Alternativ kann auch eine Authentifizierung via Tastendruck gewählt werden. Nachdem Benutzername und Kennwort in eine Applikation eingegeben wurden, wird eine SMS-Verifizierung an die mobile App gesendet. Hier kann der Benutzer den Anmeldeversuch dann freigeben oder ablehnen.

Produktmerkmale & Features

- Synchronisation von Daten und Einstellungen basierend auf einem standardisierten SCIM v.2.0-Schema
- Vereinheitlichung der Provisionierungsprozesse
- Zwei-Faktor-Authentifizierung via Tastendruck, SMS oder Anruf
- Mobile Starling 2FA-App für iOS, Android und Chrome
- Unterstützung von Federation-Protokollen einschließlich SAML 2.0 für Support-Anmeldungen bei Cloud-Anwendungen (z. B. Google Apps, Salesforce)
- ADFS Adapter
- RADIUS-Agent zur Authentifizierung via RADIUS-Protokoll
- HTTP-Agent für IIS-Websites
- Umfangreiche Audit-Trails zur Einhaltung gesetzlicher Bestimmungen

Ihr Nutzen auf einen Blick

- Automatisierte Zuweisung von Benutzerrollen, Provisionierung und Durchsetzung von IAM-Richtlinien
- Geringeres Risiko eines Sicherheitsverstoßes aufgrund kompromittierter Authentifizierungsdaten
- Verbesserte Verwaltung einer Vielzahl von Systemen im ganzen Unternehmen
- Konsolidierung der Zugriffssteuerung für hybride Systemumgebungen
- Vereinfachung komplexer Benutzerberechtigungen und -prozesse
- Realisierung von Compliance und echter IGA
- Sicherstellung einer unternehmensweiten sicheren Benutzerzugriffsrichtlinie

„Hybride und Cloud-gestützte Systemumgebungen stellen die IT-Sicherheit vor besondere Aufgaben. Unternehmen sind vor dem Hintergrund von Gesetzesvorgaben, Compliance-Anforderungen und individuellen Sicherheitsvorschriften dazu angehalten, ein richtliniengesteuertes Identitäts- und Zugriffsmanagement zu implementieren, welches über die gesamte Infrastruktur hinweg höchstmögliche Sicherheit, Transparenz und Regelkonformität gewährleistet. Mithilfe der Starling Cloud-Plattform und den dazugehörigen optionalen Services schaffen Unternehmen hierfür die verwaltungstechnischen Voraussetzungen."

Gerald Appel (Team Lead One Identity)